Boston Scientific

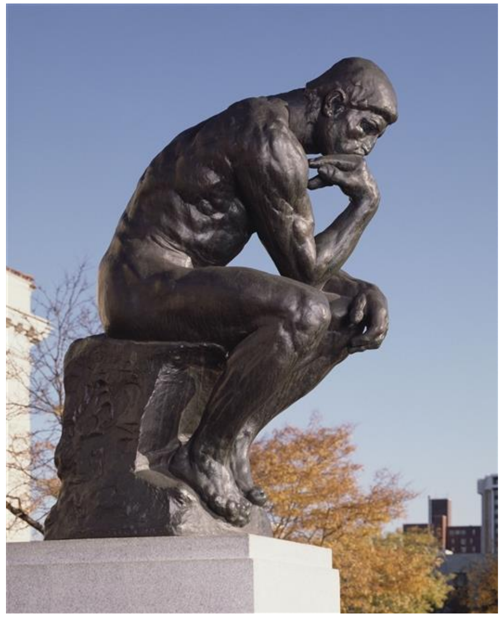
Advancing science for life™

Ruminations on challenges in securing medical devices

Ken Hoyme
Director, Product & Engineering Systems Security

What is a rumination?

- ru·mi·na·tion (ro͞oməˈnāSH(ə)n/)
  - *noun*
  - **1**. a deep or considered thought about something. "philosophical ruminations about life and humanity“



  - **2**. the action of chewing the cud. "cows slow down their rumination"

Scalability Challenges

⋮

- Allowable complexity of solutions
- Scalability of requirements
- Awareness of inventory/Bill of Materials
- Technical competencies of available staff
  - Can’t require a “PhD in the loop”

⋮

Software Inventory Challenges

Boston Scientific

- Knowledge of what 3rd party SW content is in a device is not well coordinated.
  - Device Manufacturer
  - End user
  - Different patch levels (what version changes with a device patch update?)
- Discovery tools exist, but vary in their capabilities
- HDOs legitimately want to understand their exposure when a high-profile vulnerability is exposed
  - Can you say “WannaCry” – I knew you could….
- Are there more effective ways and tools to communicate COTS BOMs (Bill of Materials) and correlation to patch levels to allow more rapid risk assessment?
  - An issued patch that has not been fully applied complicates the assessment\

Composability

- Safety and security are “emergent properties”
  - One can build safe and secure systems from non-safe, non-secure components…
  - And vice-versa…
- Individual medical devices are developed independently, and approved independently
  - Regulators are examining safety and security on a device, by device basis
- There is value in having devices integrated into networks and interconnected
  - Closed loop monitoring
  - Clinical decision support
  - Alarm monitoring systems
- How to evaluate whether an integrated system is safe and secure?
  - Who performs this analysis?
  - How is it re-evaluated when individual devices are updated?

Hybrid Usability

- Usability is also an emergent property
- Usability analysis is performed on a device-by-device basis
- If devices from different manufacturers are secured in totally different ways, what happens to the aggregate usability of them if all connected to the same patient?
  - Will a clinician make a mistake out of confusion over different security controls?
  - Can patient harm result?
- *How to evaluate whether an integrated system is usable?*
  - *Who performs this analysis?*
  - *How is it re-evaluated when individual devices are updated?*

Authentication in Real-life Clinical Settings

- How can we authenticate clinical users in all situations?
  - Badges
  - PINS
  - Passwords
  - Biometrics
- What methods work in all spaces of clinical care?
  - Infectious patient
  - Immune-deficient patient
  - Emergency care

Does "Break Glass" Break Security?

- EHR's can offer a "break glass" option
  - Subject to post-event audit
- When a device has safety implications, how can an emergency access function be offered without unacceptable risk of harm?

M2M Authentication

- Connecting devices to EHR’s and other systems requires some form of authentication
  - Manufacturer may offer a means to authenticate their device to the manufacturer’s systems
  - E.g. for software updates
- How does the HDO ensure that devices on their network are authenticated for their domain?
  - Consider leased devices that come and go …
  - HDOs that don’t want a SW update pushed until they have verified it

Lack of True Separation

- How do assure that "essential performance" of a device is maintained if communications functions are compromised?
  - Many examples of safety and security critical architectures that do this right
- There is a need for embedded device architectures that provide hard separation between processes
  - That are deployable by a wide range of device companies
  - "No PhD in the Loop"

The Allure of COTS in a Decades-long Application

- Why do we continue to use COTS with a 3-7 year life-cycle on devices with 10-15 year life-cycles?
  - And bulky COTS with a broad attack surface
- We need an OS that is
  - Simple
  - Basic communications
  - Separation
  - Underlying behavior proofs
  - Easy to program applications